UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,498	02/09/2004	Robert R. Gilman	4366-139	2317

48500 7590 05/30/2007

SHERIDAN ROSS P.C.
1560 BROADWAY, SUITE 1200
DENVER, CO 80202

EXAMINER	
AHUJA, SUPRIYA	
ART UNIT	**PAPER NUMBER**
2109	

MAIL DATE	DELIVERY MODE
05/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,498	GILMAN ET AL.	
	Examiner	Art Unit	
	Supriya Ahuja	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-62* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/09/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. **Claims 3, 9, 11, 12, 23, 33, 34, 39, 43, 52 and 53** are objected to because of the following informalities:

Claims 3, 34 and 53, lines 1 and 3, replace the phrase "a secret key" with --the secret key--, and "a registration request" with --the registration request--.

Claim 9, line 1, replace the phrase "a unique identifier" with --the unique identifier--.

Claims 11, 33 and 52, lines 1-4, replace the phrase "the digital signature" with --a digital signature-- and "the personal identification number" with --a personal identification number--.

Claim 12, line 2, replace the phrase "a key identifier" with --the key identifier--.

Claim 23, lines 11-12, replace the phrase "a key identifier" with --the key identifier--.

Claim 39, line 3, replace the phrase "the enterprise master key" with --an enterprise master key-- as it lacks antecedent basis.

Claim 43, line 10, replace the phrase "the unique identifier" with --a unique identifier--.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. **Claim 43** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In independent claim 43, the claim recites the steps for performing the functions of establishing, generating, and providing, when the authentication of the key generating agent is successful. Moreover, registering the communications device, only when authentication of the communication device is successful. However, there is no mention of the steps when the authentication is unsuccessful and is unclear as to what should be done when authentication does not take place. Therefore, the claim language needs to be corrected and explained clearly.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1, 4, 5, 12-15, 17-20, 21-24, 26-27, 35-37, 40-44, 46, and 54-62** are rejected under 35 U.S.C. 102(b) as being anticipated by Menon et al. (US 2001/0001268 dated 05/17/2001).

6. **Claims 1, 23, 43 and 60.** A method or a packet-switched communications device (It is inherent that a device comprises a processor to execute instructions) (abstract lines 18-21) for provisioning and registering a packet-switched communications device (computing devices,

[0052] lines 3-9, [0102] lines 8-14) in an enterprise network (Public Switched Telephone Network (PSTN), WAN, Internet, [0051] lines 3-7), comprising:

assigning an electronic address (IP address, [0060] line 3) to the communications device (terminal, [0060] lines 2-8);

providing the electronic address (IP address, [0060] line 3) and an address associated with a key generating agent (CPRU, [0061] lines 3-8) to the communications device;

communications device authenticating the key generating agent ([0174] lines 4-11); and

when authentication of the key generating agent is successful, performing the following functions:

establishing a secure communications session with the key generating agent [0178];

generating a secret key (secret key, [0175] lines 5-6)

i) using the unique identifier (unique universal identifier, [0175] line 7) of the communications device when a key identifier is derived using the unique identifier (It is inherent that the secret key will be derived from an identifier where the identifier can be a device ID or a user ID or a random number, etc.) or

ii) not using the unique identifier when the key identifier is derived using information not associated with the communications device (unique universal identifier, [0175] line 7); and

providing, to the communications device through the session, the secret key (secret key, [0175] lines 1-10);

an application server (RADIUS server or a gatekeeper, [0285] line 9; It is inherent that a server comprises a processor to execute instructions) receiving a registration request ([0102] lines 8-14; [100]; [0104]; [0361]; signaling information, or packets or messages, [0286] line 2; It is an

intrinsic property of the mobile terminal to register with the server by sending request in order to communicate and authenticate) from the communications device (terminals, [0286]), wherein the registration request comprises the key identifier (a registration request can be in any for of information like keys, identifiers, random numbers, etc);

the application server authenticating the communications device using the secret key (It is inherent that the server or gatekeeper authenticates the terminal using a secret pass-code or key or a public-private key); and

when the communications device is successfully authenticated (it is inherent that once the authentication is complete, the terminal is registered), registering the communications device [0102].

7. **Claims 4 and 26.** The method or device, further comprising before the establishing step:

authenticating the key generating agent key (It is inherent that the server authenticates the terminal using a secret pass-code or key or a public-private key);

performing the establishing, providing, and receiving steps when authenticating the key generating agent is successful (it is inherent that once the authentication is complete, the terminal is registered, and a connection is established, where the terminal can perform other functions in communication with the server, once authenticated).

8. **Claims 5, 27 and 46.** The method or device, wherein the secret key is a symmetric key (public key scheme using RC4 algorithm [240], where RC4 is a stream cipher).

9. **Claims 12, 17 and 55.** The method, wherein the communication device provides to the key generating agent through the session, the key identifier when the communication device computes the key identifier; the receiving step further comprises receiving, from the key

generating agent through the session, a key identifier; and the providing step further comprises providing, to the communications device through the session, the key identifier (It is a property for two devices on a network to send and receive information where the information can be in any form like a key or a key identifier in order to authenticate or register the terminal or device to access content).

10. **Claims 13 and 35.** The method or device, further comprising before the establishing step: receiving an IP address assigned to the communications device ([0060] lines 1-4).

11. **Claims 14, 36, 54 and 61.** The method or device, wherein the establishing step comprises: establishing a logical connection (access to the wireless access system, [0178] line 6) with the key generating agent (CPRU, [0178]); negotiating security parameters (identifiers or secret key); authenticating the identity of the key generating agent ([0178] lines 6-9); and when authentication is successful, activating the negotiated security parameters to establish the secured communications session [0178].

12. **Claims 15, 37 and 57.** The method or device, further comprising:
when authentication is successful, establishing secure communications [0178].

13. **Claims 18, 40 and 56.** The method or device, further comprising:
closing the secured session (closing, [0116] lines 1-3); and
computing a packet switched device authentication key (secret key, [0175] lines 5-7) using the secret key (key identifier, [0175] lines 5-7).

14. **Claims 19, 41 and 62.** The method or device, wherein the step of authenticating further comprising:

when authentication is successful, establishing secure communication with the communications device [0178].

15. **Claims 20 and 58.** A computer readable medium comprising instructions to perform the steps of Claim 1 and 43(The method of claim 1 can be implemented in the form of a software).

16. **Claims 21 and 42.** The method or device, wherein the establishing, providing and receiving steps are free of a challenge message and a response thereto (A user id/password technique and the Password Authentication Protocol (PAP) may be used instead of the challenge/response process; [0173]).

17. **Claims 22 and 59.** A logic circuit operable to perform the steps of Claim 1 and 43 (Figure 1).

18. **Claims 24 and 44.** The packet-switched communications device or the method, wherein the packet-switched communications device is unprovisioned and does not possess the secret key before the receiving function or the providing step (It is inherent that before the secret key is sent to the device, the device does not already possess the secret key).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. **Claims 2, 25 and 45** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Chan et al. (US 6128389 dated 10/03/2000).

21. Menon et al. discloses all the limitations of claim 2, 25 and 45 except that the key identifier is a function of at least one of a pseudo-random number generator, a database of keys and key identifier, and a hash function.

The general concept of using a key identifier as a function of a pseudo-random number generator is well known in the art as illustrated by Chan et al., which discloses the SAMS A-key generation/distribution unit which generates a 20-digit pseudo-random number based on a random seed (col. 10 lines 16-20, Equation 3 line 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of a pseudo-random generator as taught by Chan et al. in order to increase security.

22. **Claims 3, 34 and 53** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Rai et al. (US 6675208 dated 01/06/2004).

23. Menon et al. discloses all the limitations of claim 3, 34 and 53 except that the communications device possesses a secret key and the communications device is not in secure communications with the application server, wherein the communications device provides a registration request to the application server using the key identifier.

The general concept of using a secret key and the device providing a registration request to the server is well known in the art as illustrated by Rai et al., which discloses a foreign domain name

which is used as the key to search the foreign domain directory for an entry that matches the fully qualified domain name of the foreign registration server relaying the registration request and a shared secret used between the foreign and home registration servers to authenticate their identity mutually with each other for the wireless device (col. 35 lines 1-11).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of a registration request and a secret key as taught by Rai et al. in order to register the device with the server.

24. **Claims 6, 8, 28, 30, 39, 47 and 49** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Molva et al. (US 5347580 dated 09/13/1994).

25. Menon et al. discloses all the limitations of claims 6, 8, 28, 30, 39, 47 and 49 except that the secret key is derived from an enterprise master key and the key identifier.

The general concept of using another key and a key identifier to derive a secret key is well known in the art as illustrated by Molva et al. which discloses deriving the secret card key of the smartcard from the card identifier by encrypting the card identifier with a server secret key, storing at the server user names, user personal identifiers, and server secret key, and determining at the server the potential secret card key from the received card identifier and the server secret key (claim 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of a master key and a key identifier to derive a secret key as disclosed by Molva et al. in order to securely authenticate a device.

26. **Claims 7, 29 and 48** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Chan et al. (US 6128389 dated 10/03/2000).

27. Menon et al. discloses all the limitations of claims 7, 29 and 48 except that the enterprise master key is calculated using a seed value and a pseudorandom number generator.

The general concept of using a seed value and a pseudorandom number generator is well known in the art as illustrated by Chan et al., which discloses the SAMS A-key generation/distribution unit which generates a 20-digit pseudo-random number based on a random seed (col. 10 lines 16-20, Equation 3 line 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of a pseudo-random generator and a seed value as taught by Chan et al. in order to generate random or pseudo-random values (col. 9 lines 33-36).

28. **Claims 9, 31 and 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Kocher et al. (US 20020099948 dated 07/25/2002).

Menon et al. discloses all the limitations of claim 9, 31 and 50 except that the key identifier computed from a unique identifier comprises at least a first field comprising an identifier associated with the key generating agent, a second field comprising the identifier of the communications device, and a counter field.

The general concept of using identifiers associated with devices and a counter field to compute a key identifier is well known in the art as illustrated by Kocher et al. which discloses the content identifier can be a simple identifier, a randomly produced or cryptographically generated value a

counter, a combination of parameters, etc. and may be generated by the content provider, ICP, playback device, CryptoFirewall, etc. ([0077] lines 9-14).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of identifiers and counters to compute key identifiers as taught by Kocher et al. in order to access content (0063] lines 2-3).

29. **Claims 10, 32 and 51** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Chan et al. (US 6128389 dated 10/03/2000).

30. Menon et al. discloses all the limitations of claim 10, 32 and 51 except that the unique identifier of the communications device is at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the communications device on the enterprise network.

The general concept of using a serial number or an address of the communications device as the unique identifier is well known in the art as illustrated by Chan et al. which discloses the use of the terminal location address or terminal identifier in the A-key management system (col. 7 lines 59-67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of device identifier as the unique identifier as taught by Chan et al. in order to access content.

31. **Claims 11, 33, and 52** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Boate et al. (US 20020104006 dated 08/01/2002).

32. Menon et al. discloses all the limitations of claims 11, 33, and 52 except for digitally signing a message where the digital signature is derived from the secret key, a constant and a personal identification number of a user associated with the communications device.

The general concept of using a digitally signed message where the digital signature is derived from a secret key, a constant, a personal identification number is well known in the art as illustrated by Boate et al. which discloses the use of a biometrical (fingerprint, claim 21) digital signature used to sign a message derived by a private key ([0039] lines 34-38) (It is an obvious design choice to derive the digital signature using a secret key or a constant or a user identification or a combination of them).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of a digital signature as taught by Boate et al. in order to authenticate the user during registering of the user (claim 21).

33. **Claims 16 and 38** are rejected under 35 U.S.C. 103(a) as being unpatentable over Menon et al. (US 20010001268 dated 05/17/2001), and further in view of Chan et al. (US 6128389 dated 10/03/2000).

34. Menon et al. discloses all the limitations of claims 16 and 38 except that the providing step comprises prompting a user associated with the communications device for a personal identification number and unique identifier.

The general concept of prompting for a personal identification number and unique identifier is well known in the art as illustrated by Chan et al. which discloses a system administrator module which enables a user to set or modify the telephone number of the SAMS, to set or modify the

terminal location identifier, to add or modify a terminal identifier, to alter an administrator password, and to perform administrative functions (col. 7 lines 59-67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Menon et al. to include the use of personal identification number and unique identifier as taught by Chan et al. in order to securely authenticate the user.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Supriya Ahuja whose telephone number is 571-270-1588. The examiner can normally be reached on Monday - Thursday 7:30 -5:00; 2nd Friday 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-1808. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Supriya Ahuja

S.A.
05/23/2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER